Layers of protection

How to secure your organization and intellectual property

INTERVIEWED BY JAYNE GEST

BEN SIMMS
Vice president
Blue Technologies

(216) 271-4800, ext. 2260
bsimms@btohio.com

FOLLOW UP: To learn more about securing your company's intellectual property, contact Blue Technologies.

Smart devices and other technology tools are becoming more pervasive within all organizations. It's the internet of things taking shape; everything from smart boards and devices, to cloud computing, artificial intelligence and data acquisition.

"We're using technology to do more with less — to more effectively collaborate and communicate," says Ben Simms, vice president at Blue Technologies. "But when you do that, you open yourself up and become a little bit more vulnerable."

Smart Business spoke with Simms about how to address the growing concern of security.

Why should all business executives take security for their technology seriously?

It's incumbent upon every business leader today to look hard at where they are.

The security of your network and servers — whether on-premise, in the cloud or both — are not the only areas of vulnerability. For example, hackers were able to breach a corporation through its HVAC smart system. So, are you looking at everything, and looking at it consistently enough? Copiers used to be analog devices. Now, they are digital on and off-ramps. They are Wi-Fi enabled, and in some cases, servers sit at the bottom of their drawers.

In addition, it's not uncommon for an executive to go to a conference, jump on the public Wi-Fi, get malware and bring that back to the home office. Before you know it, that malware penetrates the email system, which then spreads organization-wide.

Everything is inter-connected and inter-related. We share so much data in so many different ways and it's only going to be become more pervasive, as networks get faster and more robust.

What's the biggest misstep you see people make when securing their organization?

Some think that if they just invest in technology like firewalls, that is enough. But most breaches happen because people and processes are out of sync. Are your employees going through awareness training? If your people aren't aware of social engineering, phishing and other tactics, even the best defense can be penetrated.

It's harder to control the behavior of people than to add hardware and software. What sites are they surfing? Where should they go? Where shouldn't they go? That type of training is important because bad actors today can embed malware in a website pop-up ad. If someone inadvertently clicks the wrong thing, they can start to get in.

What's your advice for how organizations can start beefing up their security?

There is a security breach in corporate America every 14 seconds; it's not a matter of if, it's a matter of when. What layers are you putting into place to make your organization, and your intellectual property and data, less attractive to bad actors?

Your business needs to cover the four main areas of security — network security, data encryption, access control and physical security. There are different ways that you can test those, in order to improve them. You want to take a gamut of different security tactics, techniques and strategies, such as firewalls, data encryption and multi-factor authentication, and apply those to create barriers for breaching.

In addition, ransomware has gotten sophisticated and patient. It may attack the backups first before going to the rest of the company. By the time you realize that it's happening, it's likely too late. That's why your backups should be off-site and gapped appropriately from your existing networks.

You also need to ensure your organization follows any relevant regulations for personal information that you collect, as well as security requirements in your contracts, such as manufacturing companies that must be DFARS compliant.

By working with someone who can create a customized plan for your organization, you can do an assessment to understand the current state of your security. Where are you at today? Where are your areas of vulnerability? Then, what would be a more desired state? How would you ideally make your organization less of a target? Finally, create a gap analysis and milestone deliverable to get from your current security to that desired future state. Also, if your business isn't compliant, how are you working toward compliance? Having a game plan is an important step and can go a long way to appeasing the regulatory agencies that oversee these things. ●